Misaligned Incentives

Driven by market forces, cybercriminals are outpacing defenders.

Three Dimensions Of Misalignment

Misalignment of cybercrime and response is complex. It happens at multiple levels: between attackers and defenders, between strategy and implementation, and between the executive and implementer levels of an enterprise.

Attackers vs. Defenders

Agile and quick

Attackers' incentives are shaped by a fluid, decentralized market, making them agile and quick to adapt.

VS.

Constrained by bureaucracy

Defenders are constrained by bureaucracy and top-down decision making.

Strategy vs. Implementation

90%

More than 90 percent of organizations have a cybersecurity strategy.

VS.

Less than 50%

Less than half of organizations have fully implemented their strategies.

Executives vs. Implementers

Measure success differently

Senior executives designing cyber strategies measure success differently than the implementers.

VS.

Limited effectiveness

Implementers that put strategies into practice, are limited by senior executives.

The State Of Misalignment

While cybersecurity risk is more of a concern than ever for enterprises, there are fault lines in risk management, team incentives, and inherent in how attackers operate versus how defenders manage themselves.

54%

54 percent of the executives surveyed are more concerned about reputational impact than the actual effects of a cybersecurity incident.

76%

76 percent of respondents say that cybersecurity risk is now a top three risk factor.

83%

83 percent of respondents continue to report damage due to cybersecurity breaches.

5× more likely

Operators were five times more likely to report that no incentives exist for cybersecurity.

Ideas/money

Upper-tier cybercriminals steal ideas while lower-tier criminals steal money.

51%

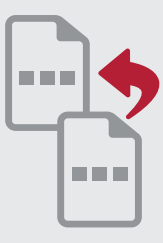
Only 51 percent of polled IT specialists in Russia had found jobs in the legitimate IT sector.

42%

As many as 42 percent of vulnerabilities are exploited by criminals within 30 days of being disclosed.

Lessons From The Criminal Market

Criminal market vs. defenders' analogue



Increase transparency

Expanding information sharing can help reduce costs to defenders by reducing duplication, and can help spread the word about new technologies and practices that deliver significant improvements in security.

Align incentives

In order to align incentives from leadership down to operators, incentives like awards and bonuses must be provided to employees and managers who deliver good security outcomes.

Leverage market forces

Outsourcing and open contracting can help reduce costs, increase competition, and promote the spread of innovative best practices.

Lower barriers to entry

Drawing on a broader talent pool, including young people and foreign ICT experts that are often drawn into cybercrime, can help fill the cyber skills gap for companies and drain talent from the criminal market.

Use public disclosure

Responding more quickly to public vulnerability disclosures through improved patching practices and faster replacement of legacy systems can enhance security and raise costs to attackers.

Get aligned. Learn from attackers. Adapt and thrive.

Visit www.mcafee.com/misaligned for the full report.

intel Security

2504_0217_info-misaligned-incentives-cybercriminals-defenders_PAIR